

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF THE NORTHERN MARIANA ISLANDS

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
GOOGLE ACCOUNTS
DOE461428@GMAIL.COM AND
SCARBALLON@GMAIL.COM THAT IS
STORED AT PREMISES CONTROLLED
BY GOOGLE LLC

Case No. **MC - 24 - 00094**

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Jason R. Oakley, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with **doe461428@gmail.com** and **scarballon@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Google LLC (“Google”), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheater Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am an investigative or law enforcement officer of the United States, within the meaning of Section 2510(7) of Title 18, United States Code.

3. I have been a Special Agent with the Federal Bureau of Investigation (“FBI”) since 2002. In that capacity, I have conducted numerous investigations into violations of federal criminal law to include domestic terrorism and threats communicated in interstate commerce. Prior to serving with the FBI, I served for nine years with the Texas Department of Public Safety as both a State Trooper and Sergeant Investigator.

4. During my time in law enforcement, I have become knowledgeable about the enforcement of State and Federal laws pertaining to terroristic threats and the means of transmitting threats via interstate commerce by use of wireless electronic communication.

5. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 115(a)(1)(B), and 18 U.S.C. § 875(c) have been committed by unknown persons. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

8. The United States, including the FBI and United States Marshal’s Service (“USMS”), is conducting a criminal investigation of an unidentified subject regarding possible

violations of Title 18, United States Code, Section 115(a)(1)(B), and Title 18, United States Code, Section 875(c).

9. On November 14, 2024, Special Agent Jason R. Oakley (“SA Oakley”) of the FBI was notified by Deputy United States Marshal Samuel Sosa (“DUSM Sosa”) of a series of harassing and threatening emails sent to United States Probation for the District of the Northern Mariana Islands. The emails were sent to the publicly available inbox at GUPml_NMI. Over 1000 emails were received from **doe461428@gmail.com**. A review of the emails revealed threats to government officials, threats to bomb Saipan, and a threat to kill United States District Court Judge Ramona Manglona.

10. On November 10, 2024, at 2:40 a.m. CHST, **doe461428@gmail.com** sent the following email to GUPml_NMI: “Okay the Federal Court House can shut down [REDACTED] [REDACTED] or let’s disappear him.” On November 10, 2024, at 9:27 p.m. CHST, **doe461428@gmail.com** sent the following email to GUPml_NMI: “Than its we know I know right right I just want to kill judge Ramona.” On November 11, 2024, at 2:03 p.m. CHST, **doe461428@gmail.com** sent the following email to GUPml_NMI: “She better not go from there or I will start bombing up saipan.”

11. On November 14, 2024, at 5:00 p.m. CHST, SA Oakley requested subscriber information from Google LLC via an emergency disclosure request. At 5:15 p.m. CHST on the same date Google LLC provided requested information indicating that **doe461428@gmail.com** was using a BLU Android phone Model G71L, Android ID 3801465288727833168, IMEI(s) 359529380156187, 359529380106182, Serial G0710WW:2010308022805612 (“Suspect Device Identifiers”) utilizing internet service provider (“ISP”) IT&E.

12. On November 14, 2024, at 6:47 p.m., SA Oakley requested subscriber information via emergency disclosure request for the Suspect Device Identifiers from IT&E. On November 15, 2024, at 10:13 a.m., IT&E provided the following information regarding the Suspect Device Identifiers: Call Number [REDACTED] with IMSI 310110670789981, a pre-paid wireless phone with no identified subscriber.

13. On November 18, 2024, at 11:16 a.m. CHST, SA Oakley was notified by DUSM Sosa that an additional email, **scarballon@gmail.com**, was sending harassing emails to GUPml_NMI with a writing style similar to that of **doe461428@gmail.com** and with multiple references to United States District Judge Ramona Manglona. SA Oakley requested subscriber information from Google LLC via emergency disclosure to request subscriber information for **scarballon@gmail.com**. Subscriber information provided by Google LLC for **sarballon@gmail.com** was identical to the Suspect Device Identifiers for **doe461428@gmail.com**.

14. A review of emails sent by **doe461428@gmail.com** showed that on November 9, 2024, at 8:04 p.m. CHST, an email was sent including the line “This is Edward Gene Worswick Richards.”

15. DUSM Sosa verified that the Transportation Safety Administration (“TSA”) at the Saipan International Airport (“SIA”) Office has an employee named [REDACTED] that was referenced in the threat dated November 10, 2024. On November 19, 2024, DUSM Sosa interviewed [REDACTED] at SIA. [REDACTED] indicated that Edward Gene Richards (“EGR”) is [REDACTED] Worswick is EGR’s mother’s maiden name. [REDACTED] told the investigating officers he believes EGR lives with his father, [REDACTED] and said that EGR suffers from mental health issues.

16. A preservation request was submitted for this account on November 18, 2024.

BACKGROUND CONCERNING GOOGLE¹

17. Google LLC (“Google”) is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

18. In addition, Google offers an operating system (“OS”) for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

19. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

20. Google advertises its services as “One Account. All of Google working for you.” Once logged into a Google Account, a user can connect to Google’s full suite of services offered

¹ The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the “Google legal policy and products” page available to registered law enforcement at lers.google.com; product pages on support.google.com; or product pages on about.google.com.

to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

21. Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses (“recovery,” “secondary,” “forwarding,” or “alternate” email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

22. Google provides an address book for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their Android mobile phone or device address book with their account, so it is stored in Google Contacts. Google preserves contacts indefinitely unless the user deletes them. Contacts can be accessed from the same browser window as other Google products like Gmail and Calendar.

23. Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user’s messages if the user has not

disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.

24. Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely unless the user deletes them.

25. Google Keep is a cloud-based notetaking service that lets users take notes and share them with other Google users to view, edit, or comment. Google Keep notes are stored indefinitely unless the user deletes them. Android device users can also use Google Drive to backup certain data from their device. Android backups on Google Drive may include mobile application data, device settings, file downloads, and SMS messages. If a user subscribes to Google's cloud storage service, Google One, they can opt to back up all the data from their device to Google Drive.

26. Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

27. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

28. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

29. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

30. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence is being sought to affirmatively identify the user of the account from which threatening communications were sent and identify their location, thus enabling the United States to establish and prove each element, or, alternatively, to exclude the innocent from further suspicion.

31. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user

attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

32. Account activity may also provide relevant insight into the account owner’s state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

33. Therefore, Google’s servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information constitutes evidence of the crimes under investigation including information that can be used to identify the account’s user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

34. I anticipate executing this warrant under the Stored Communications Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B.

Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

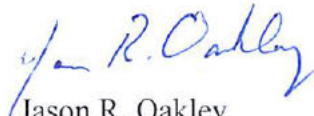
35. Based on the facts as set forth in this affidavit, I believe there is probable cause for a search warrant authorizing the search of the premises as described in Attachment A, to seek property that constitutes evidence of the commission of a criminal offense and/or property designated or intended for use or which is or has been used as a the means of committing a criminal offense, namely possible violations of 18, United States Code, Section 115(a)(1)(B), and 18, United States Code, Section 875(c).

36. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

37. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

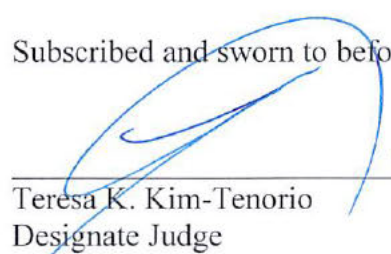
FURTHER AFFIANT SAYETH NAUGHT.

Respectfully submitted,

A handwritten signature in blue ink, appearing to read "Jason R. Oakley", is written over the typed name.

Jason R. Oakley
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on November 27th, 2024



Teresa K. Kim-Tenorio
Designate Judge